

CLEARY GOTTlieb STEEN & HAMILTON LLP

One Liberty Plaza
New York, NY 10006-1470

T: +1 212 225 2000

F: +1 212 225 3999

clearygottlieb.com

WASHINGTON, D.C. • PARIS • BRUSSELS • LONDON • MOSCOW
FRANKFURT • COLOGNE • ROME • MILAN • HONG KONG
BEIJING • BUENOS AIRES • SÃO PAULO • ABU DHABI • SEOUL

D: +1 212-225-2086
jrosenthal@cgsh.com

THOMAS J. MOLONEY
DAVID G. SABEL
JONATHAN I. BLACKMAN
RICHARD S. LINCER
JAMES A. DUNCAN
STEVEN M. LOEB
CRAIG B. BROD
NICOLAS GRABAR
CHRISTOPHER E. AUSTIN
HOWARD S. ZELBO
DAVID E. BRODSKY
ARTHUR H. KOHN
RICHARD J. COOPER
JEFFREY S. LEWIS
PAUL J. SHIM
STEVEN L. WILNER
ANDRES DE LA CRUZ
DAVID C. LOPEZ
MICHAEL A. GERSTENZANG
LEWIS J. LIMAN
LEV L. DASSIN
NEIL Q. WHORISKEY
JORGE U. JUANTORENA
MICHAEL D. WEINBERGER
DAVID LEINWAND
DIANA L. WOLLMAN
JEFFREY A. ROSENTHAL
ETHAN A. KLINGSBERG
MICHAEL D. DAYAN
CARMINE D. BOCCUZZI, JR.
JEFFREY D. KARPFF
KIMBERLY BROWN BLACKLOW
ROBERT J. RAYMOND
SUNG K. KANG
LEONARD C. JACOBY
SANDRA L. FLOW
FRANCISCO L. CESTERO
FRANCESCA L. ODELL

WILLIAM L. MCRAE
JASON FACTOR
JOON H. KIM
MARGARET S. PEONIS
LISA M. SCHWEITZER
JUAN G. GIRÁLDEZ
DUANE MCCLAUGHLIN
BREON S. PEACE
MEREDITH E. KOTLER
CHANTALE E. KORDULA
BENET J. O'REILLY
ADAM E. FLEISHER
SEAN A. O'NEAL
GLENN P. MCGRORY
MATTHEW P. SALERNO
MICHAEL J. ALBANO
VICTOR L. HOU
ROGER A. COOPER
AMY R. SHAPIRO
JENNIFER KENNEDY PARK
ELIZABETH LENAS
LUKE A. BAREFOOT
PAMELA L. MARCOGLIESE
PAUL M. TIGER
JONATHAN S. KOLODNER
DANIEL ILAN
MEYER H. FEDIDA
ADRIAN R. LEIPISIC
ELIZABETH VICENS
ADAM J. BRENNEMAN
ARI D. MACKINNON
JAMES E. LANGSTON
JARED GERBER
COLIN D. LLOYD
COREY M. GOODMAN
RISHI ZUTSHI
JANE VANLARE
DAVID H. HERRINGTON

KIMBERLY R. SPOERRI
AARON J. MEYERS
DANIEL C. REYNOLDS
ABENA A. MAINOO
HUGH C. CONROY, JR.
JOSEPH LANZKRON
MAURICE R. GINDI
KATHERINE R. REAVES
RAHUL MUKHI
RESIDENT PARTNERS
SANDRA M. ROCKS
S. DOUGLAS BORISKY
JUDITH KASSEL
DAVID E. WEBB
PENELOPE L. CHRISTOPHOROU
BOAZ S. MORAG
MARY E. ALCOCK
HEIDE H. ILGENFRITZ
KATHLEEN W. EMBERGER
AVRAM E. LUFT
ANDREW WEAVER
HELENA K. GRANNIS
JOHN V. HARRISON
CAROLINE F. HAYDAY
NEIL R. MARKEL
KENNETH S. BLAZEJEWSKI
ANDREA M. BASHAM
LAURA BAGARELLA
SHIRLEY M. LO
JONATHAN D.W. GIFFORD
SUSANNA E. PARKER
RESIDENT COUNSEL
LOUISE M. PARENT
OF COUNSEL

September 12, 2019

VIA ELECTRONIC MAIL AND ECF

The Honorable Sean H. Lane
United States Bankruptcy Court for the Southern District of New York
One Bowling Green
New York, NY 10004-1408
shl.chambers@nysb.uscourts.gov

Re: *In re BSG Resources Limited*, No. 19-11845 (SHL)

Dear Judge Lane:

We write on behalf of Vale S.A. (“Vale”) in the above-captioned proceeding (the “Proceeding”) to seek the Court’s approval of a protocol to guide disclosure of personal information under the General Data Protection Regulation (“GDPR”) in discovery (the “GDPR Protocol”).¹ Unfortunately, in the two weeks since the Parties appeared before the Court on August 29, 2019 (the “August 29 Hearing”), the Joint Administrators for BSG Resources, Ltd. (the “Joint Administrators”) and together with Vale, the “Parties”) still have not produced *any* documents despite their commitment at the hearing to produce 320 documents “next week,”² and they instead have now advised us that they are unwilling to produce any documents until the Court approves a GDPR Protocol.

The Parties have three disagreements regarding the terms of the GDPR Protocol. We have requested that the Joint Administrators produce the promised 320 documents subject to their own draft GDPR Protocol pending the Court’s resolution of the Parties’ disagreements, but the Joint Administrators have not responded to that request. Given that the parties are at an impasse on the proposed terms of the GDPR Protocol, and that the Joint Administrators have

¹ Capitalized terms used but not defined herein shall have the meanings ascribed to them in Vale’s proposed GDPR Protocol.

² August 29 Hearing Tr. 16:20; 21:7-8; 21:25.

Hon. Sean H. Lane, p. 2

now asserted this unsolved issue as their latest gating item to producing any documents, we respectfully request that the Court assist the parties by ruling on the GDPR Protocol that should be adopted in this case.

To that end, we submit herewith as Exhibit 1 Vale's proposed protocol (the "Vale GDPR Protocol"), together with Exhibit 2, a redline to the most recent GDPR Protocol we received from the Joint Administrators (the "Joint Administrators GDPR Protocol"). The three issues in dispute are:

1. the denotation of Redacted Personal Data on a specific rather than generalized basis. Vale GDPR Protocol ¶ 5.
2. whether "Personal Email Addresses" and "Nationality/Association With a Country" should fall under Category 1 of Personal Data (generally redacted) or Category 2 of Personal Data (generally not redacted). Vale GDPR Protocol, Schedule 1.
3. whether a Party redacting information under Category 2 of Personal Data should accompany such redaction with an explanation as to its necessity. Vale GDPR Protocol, Schedule 2 ¶ 4.

First, the Parties are in agreement that each document that contains Redacted Personal Data must be accompanied by a log that identifies the categories of data that are redacted. Vale contends that the log should specify a particular sub-category of Redacted Personal Data for each redaction (such that if there are multiple redactions in a document, the log would specify the sub-category for each portion redacted, such as "Home Address" and "Name of Spouse"). The Joint Administrators, however, are unwilling to associate individual sub-categories with each redaction when there are multiple redactions in a document, which would both make the review of the documents more challenging and hinder Vale's ability to formulate or assert any objection without the need for inevitable time-consuming requests for clarification. It seems self-evident that the onus should always be on the redacting Party to articulate the specific basis for each redaction in a manner that would facilitate the other Party's understanding and ability to raise an objection. Vale GDPR Protocol ¶ 5.

Second, the Parties have two disagreements as to the proper categorization of two particular subjects of Personal Data. The disclosure of Category 1 data in Schedule 1 (the "Category 1 Data") is presumed to be unnecessary to the resolution of the issues in dispute before this Court and therefore will generally be redacted. Examples of Category 1 Data include "Name of Spouse/Partner/Family Members" and "Date of Birth." Conversely, the disclosure of Category 2 data in Schedule 1 (the "Category 2 Data") is presumed to be necessary to the issues in dispute and therefore generally will not be redacted. Examples of Category 2 Data include "Directorships – Director business details" and "Business Address." In the most recent exchange between the Parties, the Joint Administrators two days ago proposed moving information about "Nationality/Association With a Country" from Category 2 Data to Category 1 Data and have added "Personal Email Addresses" to the list of Category 1 Data.

Hon. Sean H. Lane, p. 3

Nationality or association with a country is a crucial inquiry for the “center of main interest” (“COMI”) analysis and therefore, this information plainly falls within Category 2 Data that should generally not be redacted rather than presumptively redacted as with Category 1 Data. A BSGR director’s, officer’s or representative’s nationality or association with a country is important for Vale to evaluate and determine where BSGR’s business is actually conducted from and where its COMI lies. Vale GDPR Protocol, Schedule 1.

Likewise, two days ago, the Joint Administrators added “Personal Email Addresses” for the first time to the list of Category 1 Data after lengthy negotiations in which this had never been raised. Given the Court’s own recognition at the August 29 Hearing that “[i]f somebody’s conducting business of an enterprise through personal email, . . . it’s not protected as a personal email,”³ Personal Email Addresses used to send or receive documents responsive to Vale’s sustained requests for production of documents are plainly relevant and necessary to the determination of BSGR’s COMI (as well as the scope of BSGR’s document gathering responsibilities). Such email addresses are critical subjects of discovery and must not be redacted under the guise of GDPR; thus, they plainly fall within Category 2 Data.

Should the Court agree and specifically declare that the production of information concerning “Nationality/Association With a Country” and “Personal Email Addresses” is necessary for the dispute, that Court order of necessity will serve to protect the Joint Administrators from potential liability under the GDPR when they produce such data.

Third, given that Category 2 Data is presumptively necessary for the resolution of the dispute (and thus its production is authorized under the GDPR), Vale believes that any Party that nevertheless redacts Category 2 Data must accompany such redaction by an explanation as to the need for such redaction. Vale accepts that the redaction of Category 1 Data – which is presumptively sensitive and unnecessary – need not be accompanied by an explanation of necessity, but because Category 2 Data is presumptively necessary, there should be some explanation that accompanies any redaction. As the burden to justify a redaction of Category 2 Data lies with the producing party (just as the burden to challenge a redaction of Category 1 Data rests with the receiving party), without the proposed language in paragraph 4 of Schedule 2 of the Vale GDPR Protocol, that burden would effectively be reversed. Without an explanation for the redaction, the distinction between Category 1 Data and Category 2 Data is effectively blurred.

Relatedly, as part of the Court’s directive to the Joint Administrators to submit a proposed order that would provide “instruction for production quickly,”⁴ Your Honor suggested that the Court would be pleased to entertain an order that could allow the Joint Administrators to produce documents temporarily to Vale on an Attorney’s Eyes Only basis and/or allow for the recall of information if inadvertently produced in violation of GDPR.⁵ The Court also proposed that the Joint Administrators submit a proposed order that underscores the necessity of the information being produced, in order to provide the Joint Administrators with further protection in the event of a future GDPR challenge⁶ (although we believe that the Court’s July 29, 2019

³ August 29 Hearing Tr. 44:13-17.

⁴ August 29 Hearing Tr. 60:12-13.

⁵ August 29 Hearing Tr. 60:9-13; 69:13-14.

⁶ August 29 Hearing Tr. 63:7-14.

Hon. Sean H. Lane, p. 4

order denying the Joint Administrators' Motion for a Protective Order serves that purpose). In the subsequent two weeks, the Joint Administrators have declined to propose any such order either to us or to the Court, and instead have moved the negotiation of the GDPR Protocol backwards by making a new demand in their most recent draft that was not only absent from their prior draft but also not mentioned during the parties' preceding meet and confer.

Accordingly, we respectfully request that the Court order the Joint Administrators to immediately produce the 320 documents promised by them to the Court at the August 29 Hearing (with such production being provisionally subject to the Joint Administrators GDPR Protocol pending Court approval of a final protocol) and that the Vale GDPR Protocol be approved by the Court so as to prevent any further delay by the Joint Administrators.

Thank you for Your Honor's consideration.

Respectfully submitted,

/s/ Jeff A. Rosenthal

Enclosures

cc: Frederick Hyman, Esq.
Michael R. Lastowski, Esq.

Exhibit 1

Vale GDPR Protocol

This Protocol is made on

2019

BETWEEN

- (1) William Callewaert and Malcolm Cohen in their capacity as Joint Administrators (together “**Joint Administrators**” or “**Foreign Representatives**”) of BSG Resources Limited (in administration) (“**BSG**”); and
- (2) Vale S.A. (“**Vale**”)

The Joint Administrators and BSG on the one hand and Vale on the other hand together being hereinafter referred to the “**Parties**” and each being a “**Party**”.

WHEREAS

- (A) On June 3, 2019, the Foreign Representatives, on behalf of BSG, filed a *Verified Chapter 15 Petition for Recognition of Foreign Main Proceeding and Related Relief* (ECF No. 5) (the “**Verified Petition for Recognition**”) under chapter 15 of title 11 of the United States Code (the “**Bankruptcy Code**”), in the United States Bankruptcy Court for the Southern District of New York (the “**Bankruptcy Court**”) which seeks the recognition of BSG’s foreign insolvency proceeding (the “**Guernsey Administration**”) as a “foreign main proceeding” (the “**Chapter 15 Proceeding**”);
- (B) The Joint Administrators are currently represented in the Chapter 15 Proceeding by Duane Morris LLP (“**Duane Morris**”) and Vale is currently represented in the Chapter 15 Proceeding by Cleary Gottlieb Steen & Hamilton LLP (“**Cleary**”; with Duane Morris and Cleary being their respective clients’ “**Counsel of Record**”);
- (C) The Parties have served or will serve each other with, or have received from the other Party, documents, depositions, deposition exhibits, interrogatories and responses, admissions, and any other information produced, given, or exchanged by and among the Parties and any non-parties in the Chapter 15 Proceeding (“**Discovery Materials**”);
- (D) The Parties, acting through their respective Counsel of Record, have agreed to a Confidentiality Stipulation and Protective Order, which the Bankruptcy Court entered on 6 August 2019 (“**Order**”) (ECF No. 39) to assist the flow of Discovery Materials between them;
- (E) The Order confirms, amongst others, the categories of third parties with whom the Parties are permitted to share confidential Discovery Materials, including but not limited to the respective Counsel of Record; and
- (F) By this protocol (“**Protocol**”), the Parties wish to agree upon procedures for the production of documents subject to the EU General Data Protection Regulation 2016/679 (“**GDPR**”).

THE PROTOCOL SHALL BE AS FOLLOWS:

1. The following definitions apply to this Protocol:
 - a. **Business Days** means a day when banks are open for general business in both London and New York, other than Saturday, Sunday or public holiday;
 - b. **Data Protection Legislation** means the GDPR and all data protection and privacy legislation in force from time to time to which either Party is subject;
 - c. **Redacted** means anonymised, deleted or otherwise made illegible, as determined by the Party delivering the relevant Discovery Materials to the other Party;
 - d. **Supervisory Authority** means the relevant data protection supervisory authority in the territories where the Parties to this Protocol are established.
 - e. **Controller, Processor, Data Subject and Personal Data, Special Categories of Personal Data, Processing** and “appropriate technical and organizational measures” shall have the meaning given to them in the GDPR.

Redaction of Discovery Materials

2. The Joint Administrators, acting on behalf of BSG, have identified that Discovery Materials to be provided by them or on their behalf to Vale and/or Cleary (“**BSG Discovery Material**”) will in any event contain the categories of Personal Data set out in Part 1 and Part 2 of Schedule 1 and may, from time to time, contain additional categories of Personal Data. The Joint Administrators, acting on behalf of BSG, represent that they are subject to the GDPR and that all Personal Data contained in BSG Discovery Material constitutes Personal Data, the processing of which is regulated by the GDPR (“**EU GDPR Information**”).
3. The Joint Administrators, acting on behalf of BSG, represent that they have established legal grounds upon which Personal Data can be disclosed to Vale and/or Cleary in compliance with applicable Data Protection Laws and intend to redact certain Personal Data contained in BSG Discovery Materials in accordance with the redaction principles set out in Schedule 2 (“**BSG Redaction Principles**”).
4. If Vale should identify any categories of Personal Data that are EU GDPR Information contained in Discovery Materials to be provided by them or on their behalf to the Joint Administrators, BSG and/or Duane Morris (“**Vale Discovery Material**”), it shall notify the Joint Administrators and BSG accordingly and shall apply the same BSG Redaction Principles to such categories of Personal Data and this Protocol shall apply to the Vale Discovery Material, *mutatis mutandis*.
5. Where Personal Data contained in any Discovery Materials provided by or on behalf of one Party to the other Party has been Redacted (“**Redacted Personal Data**”), the redaction on the relevant Discovery Materials will contain the wording “Redacted – GDPR – Personal Data” (the “**Redaction**”). For each document with Redacted Personal Data, an accompanying log exported from Relativity will identify each Redaction and the accompanying sub-tag identifying the particular category and type of Redacted Personal

Data for that Redaction by reference to the relevant code provided in Schedule 1, as well as any “special category” data.

6. If a Party should consider the disclosure of any specific Redacted Personal Data to be necessary for the purpose of the Chapter 15 Proceeding, such Party shall notify the other Party to that effect (i) identifying the Discovery Materials and Redacted Personal Data in question and (ii) stating, in reasonable detail, the reasons why the Party receiving the Discovery Materials considers the disclosure to be necessary (“**Disclosure Notice**”).
7. A Party receiving a Disclosure Notice shall promptly advise the other Party in writing if some or all of the Redacted Personal Data cannot be provided, confirming the applicable Data Privacy Law upon which it relies and provide a brief explanation of its decision (“**Reply**”).
8. If a Party receiving a Reply should not be satisfied with the Reply, such Party may (within 3 Business Days) by notice refer the matter to the single point of contact (“**SPoC**”) of the other Party or resolution. If the matter is not resolved by the SPoCs within 3 Business Days from receipt of such notice, either Party may refer the matter to the Bankruptcy Court for resolution.

Appointment of Single Point of Contact

9. Each Party shall appoint an SPoC who will work together to seek an agreement with regard to any issue arising in connection with this Protocol, such contact to have a suitable degree of experience in data protection matters.
10. The SPoCs for the Parties shall be:

- a. For the Joint Administrators:

[Stephen Peters
55 Baker Street
London W1U 7EU
Email: Stephen.Peters @bdo.co.uk
Tel.: 44 (0)20 7893 2790]

- b. For Vale:

Samuel Levander
One Liberty Plaza
New York, NY 10006
Email: slevander@cgsh.com
Tel: 1 212 225 2951

or such other persons as may be notified by one Party to the respective other in writing from time to time.

Treatment of Personal Data Contained in Discovery Materials

11. Where Discovery Materials contain GDPR Information, the transfer of the relevant Personal Data (“**Transferred Personal Data**”) from or on behalf of one Party to the other Party (or such Party’s Counsel of Record):

- a. shall be done using secure methods and in accordance with the provisions of the Order; and
- b. shall be deemed a transfer between independent Controllers.

12. A Party receiving Transferred Personal Data (“**Transferee**”) shall:

- a. process the Transferred Personal Data only for the purpose of the preparation, assessment, conduct and administration of the Chapter 15 Proceeding (“**Purpose**”) and shall not process Transferred Personal Data in a way that is incompatible with the Purpose;
- b. ensure that it has a lawful basis under applicable Data Protection Legislation for the processing of any Transferred Personal Data;
- c. have in place appropriate technical and organizational security measures to:
 - i. prevent:
 - 1. unauthorized or unlawful access to, processing and disclosure of the Transferred Data; and
 - 2. the accidental loss, alteration or destruction of Transferred Personal Data;
 - ii. ensure a level of security appropriate to:
 - 1. the harm that might result from such unauthorized or unlawful access, processing or disclosure; and
 - 2. the nature of the Transferred Personal Data to be protected,such measures to in any event including the minimum security requirements set out in Schedule 3;
- d. ensure that its staff members are appropriately trained to handle and process the Transferred Personal Data in accordance with applicable Data Protection Legislation and are under a duty of confidentiality relating to the processing of Personal Data. The level, content and regularity of training referred to in this clause shall be proportionate to the staff members’ role, responsibility and frequency with respect to their handling of Personal Data;
- e. not retain or process Personal Data for longer than permitted by the Order and as is necessary to carry out the Purpose always provided that the Transferee shall

continue to retain Transferred Personal Data in accordance with any statutory or professional retention periods applicable in their respective country and/or industry;

- f. ensure that Transferred Personal Data is, at the election of the Party holding the Transferred Personal Data, either returned to the Party that transferred such Personal Data or destroyed once processing of the Transferred Personal Data is no longer necessary for the Purpose. Where the Party receiving Transferred Personal data elects to destroy such Transferred Personal Data it shall upon request without delay provide a certificate of destruction signed by an officer of such Party or Counsel of Record.
13. A Transferee may transfer Transferred Personal Data to third parties in accordance with the Order provided that the Transferee has in place procedures that any third party it so authorizes to have access to the Transferred Personal Data will comply with the provisions of this Protocol as if they were the Transferee (other than persons authorized or required by law or regulation to have access to the Transferred Personal Data). For the purpose of this clause 13 “transfer” shall mean any sharing of Transferred Personal Data by the Transferee with a third party, and shall include, but is not limited to subcontracting the processing of Transferred Personal Data and granting a third party controller access to the Transferred Personal Data. Cleary shall be deemed a third party of Vale under this Protocol and Vale hereby authorizes the Joint Administrators to deliver Discovery Materials directly to Cleary on Vale’s behalf.
14. If a Transferee appoints a third party processor to process the Transferred Personal Data it shall comply with Article 28 and 30 of the GDPR and shall remain liable to the Party that transferred the Transferred Personal Data to it for the acts and/or omissions of the processor.
15. The Transferee may not transfer Transferred Personal Data to a third party located outside the EEA unless it ensures that:
 - a. The transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 of the GDPR;
 - b. There are appropriate safeguards in place pursuant to Article 46 of the GDPR; or
 - c. One of the derogations for specific situations in Article 49 of the GDPR applies to the transfer.
16. The Parties agree to promptly, and in any event within 10 Business Days, provide such assistance as is reasonably required to enable the other Party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation (subject to the foregoing not causing a Party to be in breach of its obligations under the GDPR or any other applicable law, regulations or duties of confidentiality).

17. The SPoC of each Party shall be responsible for maintaining their own record in connection with requests from Data Subjects to exercise their rights under the Data Protection Legislation.
18. The Parties:
 - a. shall each (i) comply with their respective obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) data subjects under Article 33 GDPR and (ii) inform the other Party of any Personal Data Breach irrespective of whether there is a requirements to notify any Supervisory Authority or data subjects (subject to the foregoing clause (ii) not causing a Party to be in breach of its obligations under the GDPR or any other applicable law, regulations or duties of confidentiality); and
 - b. agree to provide reasonable assistance as is necessary to each other to facilitate the handling of a Personal Data Breach in an expeditious and compliant manner.
19. In the event of a dispute or claim brought by a Data Subject or a Supervisory Authority concerning the processing of Transferred Personal Data against either or both Parties, the Parties will inform each other about any such disputes or claims, and will co-operate with a view to settling them amicably (subject to the foregoing not causing a Party to be in breach of its obligations under the GDPR or any other applicable law, regulations or duties of confidentiality).
20. Each Party shall abide by a decision of a competent court of the country of establishment of the Party transferring the relevant Transferred Personal Data or a relevant Supervisory Authority.

General Provisions

21. This Protocol is drafted in the English language. If it is translated into any other language, the English language version shall prevail.
22. Any notice given to a Party under or in connection with this Protocol shall be in the English language, in writing, addressed to the SPoCs and shall be sent by email to the relevant SPoC.
23. Any notice shall be deemed to have been received by an SPoC at the time of transmission of the relevant email, or this time falls outside business hours in the place of receipt, when business hours resume. In this section 23, business hours means 9:00 am to 05:00 pm Monday to Friday on a day that is not a public holiday in the place of receipt.
24. No variation of this Protocol shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).
25. For the avoidance of doubt, the Parties' agreement to enter into this Protocol does not constitute an agreement to produce discovery in any other action or waive any defenses thereto.

Schedule 1

Categories of Personal Data

Part 1 – Category 1 Personal Data

<i>Personal Data Type:</i>	<i>Code:</i>
Names of Spouse/Partner/Family Members	1.a
Home Address	1.b
Date of Birth	1.c
ID Document details (including drivers license and/or passport details)	1.d
Bank Account details (personal)	1.e
Telephone numbers (home)	1.f
Fax Numbers (home)	1.g
Cheque Details (personal)	1.h
Data Subject's Signature	1.i

Part 2 – Category 2 Personal Data

<i>Personal Data Type:</i>	<i>Code:</i>
Name	2.a
Position / Job Title / Association / Occupation / Profession	2.b
Business Name / Company Name/ Government Affiliation / Jurisdiction / Firm Name	2.c
Directorships – Director business details	2.d
Business bio / Firm bio	2.e

Business email address	2.f
Business address	2.g
Data Subject's Initials	2.h
Telephone Number (business)	2.i
Fax Number (business)	2.j
Personal Email Addresses	2.k
Nationality/Association with a Country	2.l

Schedule 2

BSG Redaction Principles

1. Special Categories (as defined under GDPR) of Personal Data will generally be Redacted in full.
2. The categories of Personal Data set out in Part 1 of Schedule 1 will generally be Redacted in full unless disclosure of such Personal Data is necessary for the Purpose, or the Personal Data is already in the public domain.
3. The categories of Personal Data set out in Part 2 of Schedule 1 will generally not be Redacted.
4. If in limited and exceptional circumstances a Party considers it is necessary to redact any Personal Data set out in Part 2 of Schedule 1, such redaction must be accompanied by an explanation as to its necessity, set out in the Relativity log which shall accompany each such redaction.

Schedule 3

Minimum Security Requirements

- Access controls (limited to those involved in the Chapter 15 Proceeding); File restrictions (locked-down folder access)
- Destruction controls (ensuring anything excessive is destroyed at the conclusion of the Chapter 15 Proceeding and only data necessary and required is kept otherwise)

Exhibit 2

Redline of Joint Administrators GDPR Protocol

Against Vale GDPR Protocol

This Protocol is made on

2019

BETWEEN

- (1) William Callewaert and Malcolm Cohen in their capacity as Joint Administrators (together “**Joint Administrators**” or “**Foreign Representatives**”) of BSG Resources Limited (in administration) (“**BSG**”); and
- (2) Vale S.A. (“**Vale**”)

The Joint Administrators and BSG on the one hand and Vale on the other hand together being hereinafter referred to the “**Parties**” and each being a “**Party**”.

WHEREAS

- (A) On June 3, 2019, the Foreign Representatives, on behalf of BSG, filed a *Verified Chapter 15 Petition for Recognition of Foreign Main Proceeding and Related Relief* (ECF No. 5) (the “**Verified Petition for Recognition**”) under chapter 15 of title 11 of the United States Code (the “**Bankruptcy Code**”), in the United States Bankruptcy Court for the Southern District of New York (the “**Bankruptcy Court**”) which seeks the recognition of BSG’s foreign insolvency proceeding (the “**Guernsey Administration**”) as a “foreign main proceeding” (the “**Chapter 15 Proceeding**”);
- (B) The Joint Administrators are currently represented in the Chapter 15 Proceeding by Duane Morris LLP (“**Duane Morris**”) and Vale is currently represented in the Chapter 15 Proceeding by Cleary Gottlieb Steen & Hamilton LLP (“**Cleary**”; with Duane Morris and Cleary being their respective clients’ “**Counsel of Record**”);
- (C) The Parties have served or will serve each other with, or have received from the other Party, documents, depositions, deposition exhibits, interrogatories and responses, admissions, and any other information produced, given, or exchanged by and among the Parties and any non-parties in the Chapter 15 Proceeding (“**Discovery Materials**”);
- (D) The Parties, acting through their respective Counsel of Record, have agreed to a Confidentiality Stipulation and Protective Order, which the Bankruptcy Court entered on 6 August 2019 (“**Order**”) (ECF No. 39) to assist the flow of Discovery Materials between them;
- (E) The Order confirms, amongst others, the categories of third parties with whom the Parties are permitted to share confidential Discovery Materials, including but not limited to the respective Counsel of Record; and
- (F) By this protocol (“**Protocol**”), the Parties wish to agree upon procedures for the production of documents subject to the EU General Data Protection Regulation 2016/679 (“**GDPR**”).

THE PROTOCOL SHALL BE AS FOLLOWS:

1. The following definitions apply to this Protocol:
 - a. **Business Days** means a day when banks are open for general business in both London and New York, other than Saturday, Sunday or public holiday;
 - b. **Data Protection Legislation** means the GDPR and all data protection and privacy legislation in force from time to time to which either Party is subject;
 - c. **Redacted** means anonymised, deleted or otherwise made illegible, as determined by the Party delivering the relevant Discovery Materials to the other Party;
 - d. **Supervisory Authority** means the relevant data protection supervisory authority in the territories where the Parties to this Protocol are established.
 - e. **Controller, Processor, Data Subject and Personal Data, Special Categories of Personal Data, Processing** and “appropriate technical and organizational measures” shall have the meaning given to them in the GDPR.

Redaction of Discovery Materials

2. The Joint Administrators, acting on behalf of BSG, have identified that Discovery Materials to be provided by them or on their behalf to Vale and/or Cleary (“**BSG Discovery Material**”) will in any event contain the categories of Personal Data set out in Part 1 and Part 2 of Schedule 1 and may, from time to time, contain additional categories of Personal Data. The Joint Administrators, acting on behalf of BSG, represent that they are subject to the GDPR and that all Personal Data contained in BSG Discovery Material constitutes Personal Data, the processing of which is regulated by the GDPR (“**EU GDPR Information**”).
3. The Joint Administrators, acting on behalf of BSG, represent that they have established legal grounds upon which Personal Data can be disclosed to Vale and/or Cleary in compliance with applicable Data Protection Laws and intend to redact certain Personal Data contained in BSG Discovery Materials in accordance with the redaction principles set out in Schedule 2 (“**BSG Redaction Principles**”).
4. If Vale should identify any categories of Personal Data that are EU GDPR Information contained in Discovery Materials to be provided by them or on their behalf to the Joint Administrators, BSG and/or Duane Morris (“**Vale Discovery Material**”), it shall notify the Joint Administrators and BSG accordingly and shall apply the same BSG Redaction Principles to such categories of Personal Data and this Protocol shall apply to the Vale Discovery Material, *mutatis mutandis*.
5. Where Personal Data contained in any Discovery Materials provided by or on behalf of one Party to the other Party has been Redacted (“**Redacted Personal Data**”), the redaction on the relevant Discovery Materials will contain the wording "Redacted – GDPR – Personal Data." (the “Redaction”). For each document with Redacted Personal

Data, an accompanying log exported from Relativity will identify ~~the each Redaction and the accompanying sub-tag identifying the particular categories of and type of Redacted p~~Personal dData ~~set forth on for that Redaction by reference to the relevant code provided in~~ Schedule 1, as well as any “special category” data, ~~that have been redacted from such document by name or reference to the relevant code.~~

6. If a Party should consider the disclosure of any specific Redacted Personal Data to be necessary for the purpose of the Chapter 15 Proceeding, such Party shall notify the other Party to that effect (i) identifying the Discovery Materials and Redacted Personal Data in question and (ii) stating, in reasonable detail, the reasons why the Party receiving the Discovery Materials considers the disclosure to be necessary (“**Disclosure Notice**”).
7. A Party receiving a Disclosure Notice shall promptly advise the other Party in writing if some or all of the Redacted Personal Data cannot be provided, confirming the applicable Data Privacy Law upon which it relies and provide a brief explanation of its decision (“**Reply**”).
8. If a Party receiving a Reply should not be satisfied with the Reply, such Party may (within 3 Business Days) by notice refer the matter to the single point of contact (“**SPoC**”) of the other Party or resolution. If the matter is not resolved by the SPoCs within 3 Business Days from receipt of such notice, either Party may refer the matter to the Bankruptcy Court for resolution.

Appointment of Single Point of Contact

9. Each Party shall appoint an SPoC who will work together to seek an agreement with regard to any issue arising in connection with this Protocol, such contact to have a suitable degree of experience in data protection matters.
10. The SPoCs for the Parties shall be:

- a. For the Joint Administrators:

[Stephen Peters
55 Baker Street
London W1U 7EU
Email: Stephen.Peters @bdo.co.uk
Tel.: 44 (0)20 7893 2790]

- b. For Vale:

Samuel Levander
One Liberty Plaza
New York, NY 10006
Email: slevander@cgsh.com
Tel: 1 212 225 2951

or such other persons as may be notified by one Party to the respective other in writing from time to time.

Treatment of Personal Data Contained in Discovery Materials

11. Where Discovery Materials contain GDPR Information, the transfer of the relevant Personal Data (“**Transferred Personal Data**”) from or on behalf of one Party to the other Party (or such Party’s Counsel of Record):
 - a. shall be done using secure methods and in accordance with the provisions of the Order; and
 - b. shall be deemed a transfer between independent Controllers.
12. A Party receiving Transferred Personal Data (“**Transferee**”) shall:
 - a. process the Transferred Personal Data only for the purpose of the preparation, assessment, conduct and administration of the Chapter 15 Proceeding (“**Purpose**”) and shall not process Transferred Personal Data in a way that is incompatible with the Purpose;
 - b. ensure that it has a lawful basis under applicable Data Protection Legislation for the processing of any Transferred Personal Data;
 - c. have in place appropriate technical and organizational security measures to:
 - i. prevent:
 1. unauthorized or unlawful access to, processing and disclosure of the Transferred Data; and
 2. the accidental loss, alteration or destruction of Transferred Personal Data;
 - ii. ensure a level of security appropriate to:
 1. the harm that might result from such unauthorized or unlawful access, processing or disclosure; and
 2. the nature of the Transferred Personal Data to be protected,such measures to in any event including the minimum security requirements set out in Schedule 3;
 - d. ensure that its staff members are appropriately trained to handle and process the Transferred Personal Data in accordance with applicable Data Protection Legislation and are under a duty of confidentiality relating to the processing of Personal Data. The level, content and regularity of training referred to in this

clause shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling of Personal Data;

- e. not retain or process Personal Data for longer than permitted by the Order and as is necessary to carry out the Purpose always provided that the Transferee shall continue to retain Transferred Personal Data in accordance with any statutory or professional retention periods applicable in their respective country and/or industry;
 - f. ensure that Transferred Personal Data is, at the election of the Party holding the Transferred Personal Data, either returned to the Party that transferred such Personal Data or destroyed once processing of the Transferred Personal Data is no longer necessary for the Purpose. Where the Party receiving Transferred Personal data elects to destroy such Transferred Personal Data it shall upon request without delay provide a certificate of destruction signed by an officer of such Party or Counsel of Record.
13. A Transferee may transfer Transferred Personal Data to third parties in accordance with the Order provided that the Transferee has in place procedures that any third party it so authorizes to have access to the Transferred Personal Data will comply with the provisions of this Protocol as if they were the Transferee (other than persons authorized or required by law or regulation to have access to the Transferred Personal Data). For the purpose of this clause 13 "transfer" shall mean any sharing of Transferred Personal Data by the Transferee with a third party, and shall include, but is not limited to subcontracting the processing of Transferred Personal Data and granting a third party controller access to the Transferred Personal Data. Cleary shall be deemed a third party of Vale under this Protocol and Vale hereby authorizes the Joint Administrators to deliver Discovery Materials directly to Cleary on Vale's behalf.
14. If a Transferee appoints a third party processor to process the Transferred Personal Data it shall comply with Article 28 and 30 of the GDPR and shall remain liable to the Party that transferred the Transferred Personal Data to it for the acts and/or omissions of the processor.
15. The Transferee may not transfer Transferred Personal Data to a third party located outside the EEA unless it ensures that:
- a. The transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 of the GDPR;
 - b. There are appropriate safeguards in place pursuant to Article 46 of the GDPR; or
 - c. One of the derogations for specific situations in Article 49 of the GDPR applies to the transfer.
16. The Parties agree to promptly, and in any event within 10 Business Days, provide such assistance as is reasonably required to enable the other Party to comply with requests

from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation (subject to the foregoing not causing a Party to be in breach of its obligations under the GDPR or any other applicable law, regulations or duties of confidentiality).

17. The SPoC of each Party shall be responsible for maintaining their own record in connection with requests from Data Subjects to exercise their rights under the Data Protection Legislation.

18. The Parties:

- a. shall each (i) comply with their respective obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) data subjects under Article 33 GDPR and (ii) inform the other Party of any Personal Data Breach irrespective of whether there is a requirements to notify any Supervisory Authority or data subjects (subject to the foregoing clause (ii) not causing a Party to be in breach of its obligations under the GDPR or any other applicable law, regulations or duties of confidentiality); and
- b. agree to provide reasonable assistance as is necessary to each other to facilitate the handling of a Personal Data Breach in an expeditious and compliant manner.

19. In the event of a dispute or claim brought by a Data Subject or a Supervisory Authority concerning the processing of Transferred Personal Data against either or both Parties, the Parties will inform each other about any such disputes or claims, and will co-operate with a view to settling them amicably (subject to the foregoing not causing a Party to be in breach of its obligations under the GDPR or any other applicable law, regulations or duties of confidentiality).

20. Each Party shall abide by a decision of a competent court of the country of establishment of the Party transferring the relevant Transferred Personal Data or a relevant Supervisory Authority.

General Provisions

21. This Protocol is drafted in the English language. If it is translated into any other language, the English language version shall prevail.

22. Any notice given to a Party under or in connection with this Protocol shall be in the English language, in writing, addressed to the SPoCs and shall be sent by email to the relevant SPoC.

23. Any notice shall be deemed to have been received by an SPoC at the time of transmission of the relevant email, or this time falls outside business hours in the place of receipt, when business hours resume. In this section 23, business hours means 9:00 am to 05:00 pm Monday to Friday on a day that is not a public holiday in the place of receipt.

24. No variation of this Protocol shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).
25. For the avoidance of doubt, the Parties' agreement to enter into this Protocol does not constitute an agreement to produce discovery in any other action or waive any defenses thereto.

Schedule 1

Categories of Personal Data

Part 1 – Category 1 Personal Data

<i>Personal Data Type:</i>	<i>Code:</i>
Names of Spouse/Partner/Family Members	1.a
Home Address	1.b
Date of Birth	1.c
ID Document details (including drivers license and/or passport details)	1.d
Bank Account details (personal)	1.e
Telephone numbers (home)	1.f
Fax Numbers (home)	1.g
Cheque Details (personal)	1.h
Personal Email Addresses	1.i
Nationality/Association with a Country	1.j
Data Subject's Signature	1.k

Part 2 – Category 2 Personal Data

<i>Personal Data Type:</i>	<i>Code:</i>
Name	2.a
Position / Job Title / Association / Occupation / Profession	2.b
Business Name / Company Name/ Government Affiliation / Jurisdiction / Firm Name	2.c

Directorships – Director business details	2.d
Business bio / Firm bio	2.e
Business email address	2.f
Business address	2.g
Data Subject's Initials	2.h
Telephone Number (business)	2.i
Fax Number (business)	2.j
<u>Personal Email Addresses</u>	<u>2.k</u>
<u>Nationality/Association with a Country</u>	<u>2.l</u>

Schedule 2

BSG Redaction Principles

1. Special Categories (as defined under GDPR) of Personal Data will generally be Redacted in full.
2. The categories of Personal Data set out in Part 1 of Schedule 1 will generally be Redacted in full unless disclosure of such Personal Data is necessary for the Purpose, or the Personal Data is already in the public domain.
3. The categories of Personal Data set out in Part 2 of Schedule 1 will generally not be Redacted.
4. If in limited and exceptional circumstances a Party considers it is necessary to redact any Personal Data set out in Part 2 of Schedule1, such redaction must be accompanied by an explanation as to its necessity, set out in the Relativity log which shall accompany each such redaction.

Schedule 3

Minimum Security Requirements

- Access controls (limited to those involved in the Chapter 15 Proceeding); File restrictions (locked-down folder access)
- Destruction controls (ensuring anything excessive is destroyed at the conclusion of the Chapter 15 Proceeding and only data necessary and required is kept otherwise)